Functional Modelling for Fault Diagnosis and its application for NPP.

Lind, Morten; Zhang, Xinxin

Published in:
Nuclear Engineering and Technology

Publication date:
2014

Document Version
Publisher's PDF, also known as Version of record

Functional Modelling for Fault Diagnosis and its application for NPP

Morten Lind and Xinxin Zhang

Department of Electrical Engineering, Technical University of Denmark

Ørsteds Plads 349, 2800 Kongens Lyngby, Denmark

Abstract

The paper presents functional modelling and its application for diagnosis in nuclear power plants. Functional modelling is defined and it is relevance for coping with the complexity of diagnosis in large scale systems like nuclear plants is explained. The diagnosis task is analyzed and it is demonstrated that the levels of abstraction in models for diagnosis must reflect plant knowledge about goals and functions which is represented in functional modelling. Multilevel flow modeling (MFM), which is a method for functional modeling, is introduced briefly and illustrated with a cooling system example. The use of MFM for reasoning about causes and consequences is explained in detail and demonstrated using the reasoning tool the MFMSuite. MFM applications in nuclear power systems are described by two examples a PWR and a FBR reactor. The PWR example show how MFM can be used to model and reason about operating modes. The FBR example illustrates how the modeling development effort can be managed by proper strategies including decomposition and reuse.

Keywords: Fault Diagnosis, Model Based Reasoning, Artificial Intelligence, Decision Support

1. Introduction

The development of advanced methods for fault management in Nuclear Power Plants plays an important role in increasing the safety and reliability of nuclear plant operations. Recent surveys by IAEA [1] compare methodologies currently considered by the nuclear industry for fault detection, identification, diagnosis and recovery. Most of the methods rely on advanced signal processing or artificial intelligence techniques and can be used to increase the level of automation in fault management. However, in fault situations with potentially serious consequences for the plant or the environment operators are often responsible for taking action. Fault management tasks can therefore only be automated to an extent depending on the risk involved and whether the operator has a possibility to take action. Experience from the nuclear industry show that bad HMI design increases the risk of human error. The design of the human machine interaction and decision support is therefore of considerable importance in addition to automated functions for fault management.

The fault management task comprises several subtasks including monitoring, fault detection, identification, diagnosis and fault recovery. In the paper we will focus on diagnosis which is a critical step in the overall management of faults and we will consider methods suitable for handling faults in complex systems like nuclear power plants. The purpose of diagnosis is to identify causes and consequences of a given fault situation. This task is knowledge intensive and can be very demanding in dynamic situations. Advanced methods for diagnosis therefore often apply modelling techniques for representation of plant knowledge relevant for diagnosis.

The aim of the paper is to describe a modeling technique called functional modeling and explain how it can be used for diagnosis of complex system like nuclear power plants. The paper is divided into four parts. The first part comprise the remainder of the introduction and provides a brief survey of methods for diagnosis explaining the special features of functional modelling into context of other methods. The second part presents a general analysis of modeling requirements for diagnostic tasks which serve as a demonstration of the relevance of functional modelling for diagnosis of complex systems. The third part provides an introduction and demonstration of Multilevel Flow Modelling (MFM), an explanation of the basic principles of diagnostic reasoning in MFM and a demonstration on a simple cooling system example. The last part describes results from two nuclear power plant applications of MFM.

MFM has been developed over a long period of time and many publications are available describing different aspects of its application, also within nuclear power systems. The purpose of the present paper is to present previously unpublished work which provides a broader background and motivations for using MFM for diagnosis (especially parts 1 and 2), and for handling the modeling requirements in complex systems like nuclear power plants (part 4). The reader is referred to the references for details.

1.1 Methods for Fault Diagnosis

Methods for fault diagnosis use a variety of techniques which have their origin in signal processing and artificial intelligence and are sometimes classified accordingly. However, such a classification is not suitable for explaining the merits of functional modeling for fault diagnosis, the subject of the present paper. A more useful classification is a distinction of methods according to the nature of the plant knowledge used for fault diagnosis. Such a classification of methods is proposed by IAEA [1] and is a convenient starting point for explaining the significant features of functional modeling.

1.1.1 The IAEA classification

The IAEA classification includes methods currently (2008) considered in Nuclear Engineering and makes the following overall distinctions

- Empirical modelling
- Physical modelling
- Related techniques including fuzzy logic and multilevel flow modelling

We will shortly discuss this useful, but still problematic, classification in order to highlight the significant features of functional modeling. Here it is included in “related techniques” by Multilevel Flow Modelling, which is a method for functional modeling proposed by the first author [2]. The IAEA classification is problematic because the third category is simply a residual containing methods not belonging to the first two categories. Significant features of all the methods mentioned is therefore missing in the classification. A main aim of the first part of the present paper is to explain the principles of functional modelling so its distinctive features compared with both empirical and physical modelling and its potential applications for fault diagnosis in nuclear power plants become

clear.

1.1.1.1 Empirical modelling

Empirical methods use pattern recognition techniques to compare plant observations with previously identified fault situations and have been used both for fault detection and diagnosis. An advantage of empirical techniques is the independence of detailed knowledge of plant behavior. However, a disadvantage is that fault situations are defined by patterns of observed plant variables values. It may accordingly be difficult to diagnose faults which have not been encountered before. The pattern recognition algorithm may fail because it is fitted to the empirical data and a learning approach is required. Empirical modelling includes also fault trees and consequence trees which are produced as results of fault analysis and both used in off-line applications for risk assessment and for on-line applications for identification of failure causes and consequences. A significant problem with empirical methods is that faults are defined by expert judgments i.e. there is no systematic basis for defining faults and thereby to ensure completeness or consistency.

1.1.1.2 Physical modeling

Methods based on physical modelling use first principles i.e. laws of physics and chemistry. The models are used for fault diagnosis by analyzing deviations between observations and plant parameters estimated by the model. In this way the physical models compensate for lack of measurements and contribute to a higher accuracy in fault diagnosis. When using methods based on physical models a fault is defined as a deviation from a model which represents what is considered to be normal. An advantage of methods based on physical modelling is that faults can be defined in a more rigorous way compared to empirical methods. However, defining the normal by the behavior of the model and faults as deviations from the model put an unnecessarily severe restriction on the definition of faults and what is considered as normal. Faults cannot be seen as logical complements of the behavior specified by a physical model since their definition include consideration of norms and requirements. Requirements are described by constraints on physical entities, but their relations do not follow the first principles of physics and chemistry. Functional modelling described below represents requirements and their relations by goals and functions and provide therefore a more satisfying framework for definition of faults.

1.1.1.3 Related techniques

This is a residual category as mentioned above and includes two methods “fuzzy logic” and “multilevel flow modeling,” which does not have much in common, except that they are both results of artificial intelligence research in knowledge representation and reasoning. The purpose of fuzzy logic is to deal with vagueness and uncertainty in reasoning whereas the purpose of functional modelling is to represent systems as purposeful entities. Fuzzy logic may actually be used to cope with reasoning about uncertainty in functional modelling (as with other types of knowledge) but this combination is no reason to see them as belonging to the same category. We will not discuss fuzzy logic further here.

1.1.2 Functional modeling – a missing category

It is actually more relevant to compare functional models with physical models. The purpose of physical models is to represent the physical constraints of the system which determine its behavior when subject to changes in selected inputs. The purpose of functional modelling is to represent constraints between the goals and the functions of the system and its subsystems i.e. the means and the ends which define how it is operated. The conceptual basis of functional modelling is means-end and action concepts whereas the basis of physical modelling is the theory of dynamic systems and physics. A significant feature of functional modelling is its definition of faults as deviations from goals and purposes or intentions. As shown below, this definition of faults matches very well with a general understanding of the fault diagnosis problem in complex systems like nuclear power plants. We see accordingly functional modeling as defining a separate model category which is missing in the IAEA classification.

Functional modelling can be considered as a type of first principles model. But the first principles are not given by laws of nature, but by necessary logical constraints between faults, goals, tasks and plant functions and execution of actions. These principles reflect conditions for successful action and following Polanyi [5] we call them *first principles of operation*. Each condition for successful action in functional modeling define a failure type, and since functional modelling (MFM) support formal causal reasoning it provides a systematic framework for fault diagnosis.

Another significant difference is that functional modelling is qualitative by representing logical relations between means and ends whereas physical modelling is quantitative by representing relations between the values of plant variables. This means that functional modelling and physical modelling differ in two aspects: 1) by the nature of the knowledge represented (goals and functions versus behavior) and 2) by the distinction between qualitative and quantitative.

Below we will show that functional modelling also can be contrasted with empirical modelling because we can see fault and consequence trees as empirical shallow representations of the deep knowledge represented in functional models.

2 Modelling for Fault Diagnosis

To provide further motivations for using functional modeling in diagnosis we will shift the focus from the models currently used for fault diagnosis in NPP to a more general analysis of the fault diagnosis task. In particular, we will discuss how the task influences the levels of abstraction used in the model. A model is a tool and its level of detail and abstraction must comply with the needs of the diagnosis task. Overall, this means that a model for diagnosis must represent system features, so that information from plant measurements can be related to possible plant failures and possible remedial actions. These requirements to models for diagnosis are well understood, but it is in general difficult to translate the requirements into a model. The main problem is a general lack of explicit principles for construction of models for diagnosis.

As mentioned above, a widely used principle for diagnosis is to use empirical models representing relations between plant fault states, their causes and their consequences. Several modelling tools have been developed for representing fault trees and cause consequence diagrams. However, the modeling tools do not assist the engineer in addressing the interpretation problem in the selection of model

content i.e. to decide what is relevant to represent for a particular reasoning task and for a specific plant. The model builder is therefore faced with a difficult interpretation problem, and the identification of failure causes and consequences to include in the empirical model is far from trivial.

These interpretation problems in building empirical models for diagnosis will be analyzed below using a fault analysis example of an industrial process. Results of the analysis indicate that the construction of a fault tree of the process is based on an extensive body of background knowledge of diagnostic strategies, and of plant knowledge that can be organized in the means-end modeling framework provided by functional modeling. The plant operational knowledge captured in functional models is therefore more generic than the empirical knowledge represented in a fault tree.

2.1 Interpretation Problems

The overall purpose of diagnosis is to interpret the significance of deviations in plant states from their expected values. Usually, several interpretations are possible depending on the specific diagnostic goal that may be dependent on the situation. Three main types of diagnostic goals can be distinguished.

1. In some situations the diagnostic goal is to relate the symptoms of plant malfunction to a possible failed component or subsystem with the aim of repairing or exchanging the failed component. It is clear that such a goal would only be acceptable, if the plant supervisor (human or machine) is allowed to take the failed entity out of service and has sufficient time available for repair.

2. These conditions are not met if there are no spare parts or if overall requirements to plant production cannot be satisfied during the period of repair. In such situations it would be necessary to find means of compensation for the failure that avoid the removal of the failed component. It could be by using components or subsystems which can provide the function of the failed entity. The diagnostic goal is accordingly here to ensure that the plant operational goals are maintained in spite of the fault.

3. However, in situations with high risk and uncertainty it can be a dangerous decision to repair or to compensate the fault. Under such circumstances the goal of the diagnosis should be to derive and evaluate possible consequences of the failure and to provide protective action (e.g. shut down). In this case the decision to act could be done without knowing the prime cause of the failure. Taking into account the uncertainty and the possible risks the best strategy is accordingly to avoid a possible disaster by changing the operational goals of the plant.

These examples illustrate the variety of diagnostic problems that typically should be handled by operators or automated systems in the supervision of industrial plants. In order to satisfy the demands the supervisor must maintain an overview and analyze the situation in order be able to make a decision on what strategy to follow and how to act. Skilled operators that can keep the plant running under a variety of disturbance situations, have apparently the ability to adapt their diagnostic activities to the actual plant operating situation. This capability is difficult to model and simulate in artificial intelligence programs because of the range of situations to be considered and because of the difficulties of defining the strategies that control the interdependent concurrent reasoning processes

that are involved.

The modelling problem is further complicated because the plant knowledge required for diagnosis would be dependent on the diagnostic goal. If the goal is to repair the failed component, knowledge of components and their locations would obviously be required. If the goal is to compensate for the failure there would be a need for knowing possible redundant standby components or other means to remediate the failure. If the goal is to protect the plant, knowledge about possible means of protection would be required. The plant knowledge to be used is therefore dependent on the task to be solved, i.e. it is determined by an interpretation of the plant physical features within a task context.

2.2 Fault Analysis

In order get an insight in the nature of these modelling problems we will study the problems involved in fault analysis and fault tree construction. These problems may seem to have only indirect relevance for the interpretation problems in plant supervision discussed above and will therefore be explained briefly.

A fault tree is a logic description of the empirical relations between a top event or state and its possible failure causes (Fig. 1 show an example to be discussed later). A fault tree has two interpretations - a mathematical and a factual [4]. In the mathematical interpretation, elements of the fault tree (i.e. the boxes and the gate symbols) refer to propositions and logic operators i.e. mathematical concepts. The mathematical interpretation is only dependent on the logical structure of the fault tree and is sufficient for making logic inferences. It is independent of the plant states that are referred to by the propositions i.e. of the factual interpretation of the fault tree.

It is the problem of assigning factual content to the propositions in the fault tree which is of interest in the present paper. But a fault tree does not contain explicit information about the criteria used to select plant fault states or the strategy used to derive their interdependencies. This information is given by a factual interpretation of the fault tree and depends as shown below by an example both on plant knowledge and on the diagnostic strategy used.

2.2.1 A Ship Engine Cooling System Example

The following analysis of the example fault tree (Fig.1) of a ship engine cooling system (Fig.2) reveals the implicit knowledge. The aim of the analysis is to reconstruct the interpretation required to build the fault tree. In this way we will identify the diagnostic and plant knowledge that serves as a background context for the model. We will also show that this background knowledge can be represented using functional modeling.

The cooling system is used in e.g. ship diesel engines [5] and consists of two water circulation loops connected by a heat exchanger. The primary purpose of the heat exchanger is to transfer energy from the engine fresh water circulation loop to the seawater circuit and a secondary purpose is to prevent the seawater from entering the engine construction. Similar principles are used in core cooling systems for pressurized nuclear power reactors. Here the primary purpose is also cooling but the secondary purpose is to prevent the release of radioactive materials from the core to the environment. In order to simplify the analysis we will ignore plant incidents that require protective actions i.e. shut

downs or emergencies. An example of such a situation could be a sudden loss of primary coolant water in the engine slightly similar to a LOCA in a nuclear power reactor. We have selected the ship engine cooling system because of its relative simplicity and because of its similarity with the principles of NPP coolant systems.

The purpose of the cooling system is to keep the temperature of the engine within acceptable limits. Too high temperatures of the cylinders of a diesel engine can lead to breakage of the cylinder linings. A consequence of such failure can be loss of propulsion, a serious condition for a ship in narrow waters or with high traffic. The cooling system is therefore equipped with both a redundant flow path for the seawater and a water tank that can function as an independent auxiliary cooling system in the case that both seawater flow paths fail. The stop valves are used to switch and configure the system for different cooling modes. Three modes are provided: 1) a normal mode where pump P2 deliver the driving pressure, 2) a standby mode using the redundant seawater pump P3 and 3) an auxiliary mode where the water in the tank is forced through the secondary side of the heat exchanger by gravitation. For each of these modes the stop valves have different positions (open or closed). The positions of the stop valves in Fig. 1 correspond to the normal mode.

In the fault analysis it is assumed that the pump motor has stopped running. This fault may have a variety of consequences due to the physical interactions in the plant as shown in the fault tree in Fig. 1. Note that the fault tree is incomplete and it is therefore indicated that there may be several possible causes for each event in the tree. The fact that each event may have several consequences is also ignored. These simplifications are not critical here since the focus is on the problems in identifying the plant states that should be included in the fault tree.

The model proposed is representative of how fault and consequence trees build by an expert doing fault analysis would look like. But it is not entirely obvious how to account for the criteria used in the selection of the initial event and its consequences. As an example; why is “Motor has stopped“ selected as the initial event (cause) and why is ‘Pump P2 is not doing mechanical work’ selected as its consequence? The initial event could also have been described as ‘current in motor windings is zero.” In principle there are an infinite number of possible changes in the state of the motor and its subsystems and these could be included depending on the level of resolution of the description in time and space. However, not all changes would be significant for diagnosing the plant, and only significant changes of plant state should be included in the fault tree.

The following analysis will show that knowledge about the diagnostic goal and about the goals and functions the plant and its subsystems can motivate the content of the model. Usually this knowledge, that can be represented using a functional modelling method like MFM, is not made explicit in fault tree analyses. The factual interpretation of the fault tree, i.e. its references to aspects of the physical world, is therefore dependent on implicit knowledge of the intentions of the engineer or operator of the plant. The building of fault trees is accordingly dependent on implicit assumptions about plant purposes and operational principles.

The analysis of the fault tree will be done in two phases. The first critical step is to hypothesize an objective for the diagnosis. If no assumptions are made about the use of the information in the fault tree, i.e. its significance for the diagnostic problem, we cannot motivate the choice of fault states. In

the second step of the analysis it will be shown that the orientation of diagnosis towards remedial action make the knowledge of the purposes of plant components and subsystems indispensable for the interpretation of the fault tree, i.e. for the definition of its factual meaning.

2.2.2 The Diagnostic Task and Fault Tree Content

The overall purpose of diagnosis is to give directions for remedial action. There must therefore be a correspondence, directly or indirectly, between states in the fault tree and possible actions on the system. If such correspondence is absent, the model does not give information that is relevant to a solution of the fault remediation problem. As an example, there is no direct corresponding remedial action in the cooling system in Fig 1. to the state ‘the current in the motor winding is zero” because it is not possible to influence the current directly. It should be done through manipulation of parameters which are under control such as the start button. This state is therefore excluded from the model. However, the correspondence between plant events and remedial actions requires more analysis of predictive aspects and evaluative aspects of the fault trees as shown below.

The temporal development of disturbances in dynamic systems plays an important role in fault diagnosis, because the choice between alternative courses of remedial action is dependent on knowledge about the effects of a disturbance. If effects of the disturbance are not known, many alternatives of action may be possible and the supervisor is faced with an incompletely defined decision problem. The supervisor must therefore make predictions of plant states and the model used for diagnosis must therefore have a predictive capability. The fault tree in fig. 1 clearly satisfies this requirement since the states are interconnected in a causal chain from bottom to top.

Not all effects of a plant disturbance have consequences for the plant operation. Only effects that threaten the plant operational goals and constraints should be considered because they trigger remedial action. The predicted effects of disturbances must therefore also be evaluated i.e. their consequences for the plant operation must be derived.

In order to identify the content of the fault tree in Fig. 1 the sequence of fault states are analyzed in Table 1. Each row in the table comprises corresponding sets of fault states, plant goals, remedial tasks and actions to be executed (note that each row represents different interpretation of the same observation that the pressure drop across the pump is zero). The diagnostic process involves reasoning about the information in the columns in each row and between the rows. The table therefore combines plant operational goals (i.e. the plant states to be obtained) with goals of the supervisor, i.e. what to do. Supervision goals are called tasks here in order to avoid confusion caused by the use of the goal concept in different meanings. A goal can refer to a desirable future state of the plant (the meaning used here) or it can refer to a future state of doing of the action that produces the desirable plant state.

2.2.2.1 Relations between States and Plant Goals

From the first two columns, relating states and goals, it is seen that for each fault state there is a corresponding violated plant goal. The states are accordingly included in the fault tree because they describe states of significance to the achievement of plant goals (violations of plant constraints may also have been included in the example). The states represent therefore interpretations of the plant

situation corresponding to each goal.

2.2.2.2 Relations between States, Tasks and Actions

The way in which plant states are described depends also on the knowledge of the means provided by the plant designer to reach the goals i.e. the possible actions and the plant equipment available. These dependencies exist, because each state in the fault tree describes the lack of a means of goal achievement. The remedial tasks and actions can therefore be derived from the state description and knowledge about means-end relations in the plant. This will be shown below by an analysis of each level in table 1. A full demonstration of all details in the relations between fault trees and means-end models is not possible here, only indications will be presented. For convenience we will only consider levels 4, 3 and 2.

Level 4. S4 defines the plant state as a situation where the energy removed by the cooling system has been lost. The removal of the energy by the cooling system is a mean for maintaining the energy balance (which again is a condition for keeping engine temperature within limits (G4)). The loss of engine cooling can be therefore remedied by producing energy balance, which is the proposed task T4.

Level 3. S4 describe the plant state as a situation of a loss of seawater flow. The goal G3 specifies the production of a coolant flow. In the context of G3, the function of the seawater is to be a coolant i.e. to carry the energy transported by its circulation. Since the flow of seawater is lost, the cooling function is no longer available and the remedial task T3 is to produce flow of coolant by some other means. Since another commodity can be used as a coolant, namely the water in the tank, the action A3 is executed. A3 comprises two parts, a reconfiguration of the circuit and the startup of the auxiliary cooling system (opening control valve C4). The reconfiguration provides the conditions for the use of the tank and the associated piping as a transport path for the water in the tank. T3 involve switching of stop valves S1, S3 and S5 to produce conditions for path availability. On level 3, the remedial action is decided by knowing that the tank water serves the same function as the seawater and that the tank and the piping can serve as a means of mass transport in a field of gravity.

Level 2. When the goal in view is that pressure is produced (G2), the plant state is described as a failure of the pump to perform work on the coolant (S2). The pump P2 is a means of producing pressure on the fluid. Since P2 is not able to work on the fluid (the pump motor has stopped) another mean of pressure production must be used in order to remediate the situation (T2). The remedial action A2 is to put in service and use the stand-by pump P3, serving the same function as P2. A2 comprises a circuit reconfiguration task (switching of stop valves S1, S2 and S3 and S4 to pro-duce conditions for starting P3) and the start of P3. On this level, the action is decided on the basis of knowing that P2 and P3 have the same function.

2.2.2.3 Relations between the Levels

The discussion above did not consider the relations between state descriptions at the various levels. As mentioned previously, the states provide different descriptions of the same plant situation and are relate to decision contexts with different goals and associated tasks and actions in supervision of the plant operations. In addition to these ‘horizontal’ dependencies, the states in Table 1 are related

‘vertically’ through causal links. Thus, if the pump stops the pump P2 is not doing mechanical work on the seawater. This, in turn, will cause the circulation in the seawater cooling circuit to fail. Finally, the engine will lose cooling. The fault states are in this way connected by cause-effect relations that gives the fault tree its predictive capability.

However, each state has also an evaluative content because it is derived by evaluating the consequence of the state on the level below for the goal in view. Thus, S4 is the consequence of S3 in view of G4, S3 is the consequence of S2 in view of G3, and S2 is the consequence of S1 in view of G2,

The relations between levels reflect both the chains of cause and effect and the organization of the functions of the engine cooling system in a means-end chain. The sequence of levels (1, 2, 3, 4) therefore determines the order in which the different state descriptions become relevant for an understanding of the plant situation and the order in which the possible courses of action are effected. MFM models represent this knowledge of causal relations by the linking of functional levels via means-end relations.

2.3.3 Summary of the Analysis

In summary, the analysis shows that the derivation of the fault tree state sequence is based on two sources of plant knowledge: 1) knowledge about the physical causal mechanism of the cooling system and 2) knowledge about goals and functions of the ship cooling system and its subsystems and components. It can be concluded from the analysis that the reasoning required to correlate states and goals with tasks and actions on all levels depends on knowing the functions provided by plant components and subsystems for goal achievement. These relations are implicit in the fault tree but can be represented explicitly in a functional model like MFM as demonstrated below

Due to the four interpretations of the plant situation there would be four ways to respond to the failure depending upon the goal to be pursued. The selection between these alternatives depends on the multiple interpretations of the plant state, the time available for remediation and the priorities of the individual goals. All levels of interpretation are therefore required in order to make a qualified diagnosis. If levels are ignored, it will not be possible to consider alternative courses of action, i.e. the reliability of plant operations will be reduced (more shut-downs). Furthermore, if levels are ignored the risk of making the wrong decision will be increased. We need therefore plant models which can provide multiple interpretations. This is a key feature of Multilevel Flow Modeling.

3 Multilevel Flow Modelling

Multilevel Flow Modeling (MFM) is a methodology for functional modeling of industrial processes on several interconnected levels of means and part-whole abstractions. The basic idea of MFM is to represent an industrial plant as a system which provides the means required to serve purposes in its environment. MFM has a primary focus on representation of plant goals and functions and provide a methodological way of using those concepts to represent complex industrial plant. The basic idea of MFM was conceived by the first author [2] and has been developed and used over the years by his research group and by research groups in several other countries including Sweden, USA, Japan and

China. Early MFM research originated in problems of representing complex systems in human machine interfaces for supervisory control. But it has since developed into a broader research field dealing with modeling for analysis, design and operation of automation systems for safety critical complex plants. Recent introductions to MFM and various aspects of its applications are presented in [6, 7, 8, 9, and 10].

3.1 Concepts of Multilevel Flow Modeling

Concepts of means-end and whole-part decomposition and aggregation play a foundational role in MFM. These concepts enable humans like systems engineers and plant operators to cope with complexity because they facilitate reasoning on different levels of abstraction. The power of means-end and part-whole concepts in dealing with complexity has roots in natural language. But natural language is not efficient for representing and reasoning about means-end and part-whole abstractions of complex physical artifacts. MFM development draws on insights from the semantic structure of natural language but is designed as an artificial language which can serve modeling needs of complex engineering domains which cannot be handled within the common sense limitations of natural language.

Functions are represented by elementary flow and control functions interconnected to form functional structures representing a particular goal oriented view of the system. The action theoretical foundation which is under development see MFM functions as instances of more generic action types [8]. The views represented by the functional structures are related by means-end relations and comprise together a comprehensive model of the functional organization of the system.

The basic MFM modeling concepts are shown in Table 2 and comprise objectives, flow structures, a set of functional primitives (flow functions and control functions), a set of means-end and influence relations representing purpose related dependencies between functions and objectives and among the functions themselves. The functions, the functional structures and the relations are interconnected to form a hyper-graph like structure. The symbols used to represent functions, objectives, functional structures are shown in Table 2 together with symbols used for representing means-end and influence relations.

3.1.2 Fundamental features of MFM models

A particular feature of MFM is a clear separation of plant components and functions. This means that the same component or subsystem may be represented by several functions and a function may be realized by alternative components or subsystems. These many-to-many mappings between means (components or subsystems) and ends (functions) are explained in detail in [11]. The PWR model presented below includes several examples of one to many mappings between components and functions.

3.1.3 Principles and tools for building MFM models

Building an MFM model is not a simple task. First of all the model builder must have a good general knowledge about the plant and how it is operated. But the model construction is an iterative process and there is a need for strategies to help in the development and for support tools [12]. The MFMSuite

[13] under development by DTU and OECD Halden includes a graphical editor with library facilities supporting reuse during the modeling process.

There are two basic principles for building MFM models. According to the first principle, the building of a model takes its departure in the definition of objectives of the modeling object or system. System functions provided to achieve the objectives are then identified. The purpose of this top down procedure is to ensure that functions are defined in the context of system objectives. The procedure is suitable in particular for modeling systems where the physical realization is not known in detail or taken into account such as in the early phases of system design. The second principle is to associate functions with system components i.e. the physical realization. These functions are then aggregated so that they match with the objectives of the system. This bottom up the procedure is suitable when the plant objectives are unknown or vaguely defined. The aggregation process serve here to suggest possible objectives and higher levels functions in the system which cannot be directly associated with physical components or subsystems.

In most cases the two basic principles are combined into an iterative procedure. The model of the ship engine cooling system presented below is the result of such an iterative procedure. For more complex modelling tasks such as the nuclear power PWR and FBR cases presented below such a modelling procedure becomes rather time consuming if not done by an expert. An obvious way to reduce the modelling effort is to reuse model components from a library of tested and validated models. Another means of reducing the modeling effort is to use decomposition strategies for breaking down the system in to subsystems and then build the MFM models by combining MFM models of the subsystems. This strategy is exemplified in the FBR example presented below. The combination of MFM sub-models is not a trivial task because of the many to many mappings between physical structure and function, and the adaptations which may be necessary when a model component is used in a new context.

3.1.4 MFM modelling of the ship engine cooling system

An easy way to understand how MFM concepts are used is to consider the modeling of the ship engine cooling system presented in Fig. 2. By this example we can explore a large fraction of the concepts shown in Table. 2. The interested reader can find other examples described in [6].

The MFM model of the ship engine cooling system is based on the system description presented in section 2.4 and the modelling principles in section 3.1.3. The purpose of the system is to prevent overheating of the ship engine. This purpose is achieved by transporting the heat (energy) generated by the engine by means of through two cooling loops to the sea. The energy transportation is in turn obtained by using two cooling loops. Two pumps are used to move the freshwater and the seawater in the two cooling loops. This overall description of the means and the ends of the system gives a general outline for modelling the system using MFM and can be represented diagrammatically as shown in Fig. 3.

With this overall model as a basis we can develop an MFM model using several steps of iteration and refinement. The model is shown in Fig. 4.and explained below.

The objective of the system represented by «obj1» is to maintaining the removal of heat from the energy source. The energy flow structure «efs1» represent the transportation of energy from the engine (the energy source «sou1») to the sea which is an energy sink «sin1». The heat storage capacity of the system is represented by an energy storage «sto1» (the open sea water loop does not have the storage function in this case). The balance function «bal1» represents the function of the heat exchanger.

The mass flow structures «mfs1» and «mfs2» model represent the mass functions of the closed fresh water loop and the sea water loop respectively. Note that in the present model we do not consider injection of coolant water and venting. Therefore, the closed loop fresh water circulation is represented by a storage function «sto3» and a transport function «tra6» connected into a loop. The mass functions of to the sea in «mfs2» are considered as both an unlimited mass source «sou2» and a sink «sin2». Sea water is delivered from the source to the sink by two alternative transport function «tra5» and «tra10», representing the functions of the main pump P2 and the alternative pump P3. In addition to the sea water, an auxiliary cooling system serves as another water source «sou3» in «mfs2». Storage «sto4» represent the function of the water tank of the auxiliary system.

The energy flow structure «efs2», «efs3», and «efs4» represent the energy conversions within the three pumps. The energy conversion functions of a pump are described already in detail elsewhere (e.g. [6]) and will therefore be omitted here.

Flow structures can be connected with different means-end relations in MFM. For example, «tra4» in «mfs1» represent the function of pump P1 which is water transportation, which is the primary means of mediating the energy removal from the engine to the coolant loop «tra1». Similarly, «tra6» in «mfs2» is linked to the energy level by a mediate relation to «tra3» representing the energy transport from the heat exchanger to the sea. The energy levels for the different pumps can also be linked to their target (transport) functions on the material level.

One may notice that different so-called casual roles are used between adjacent flow functions within the flow structures. These casual roles do not represent flow functions or direction of flow (which is indicated by the arrow in the transport functions). They indicate how state of a function state influence its upstream or downstream functions indicated by the flow directions. The casual roles will be explained after the introduction to MFM reasoning below.

3.2 Using MFM for Diagnostic Reasoning

MFM modelling is not only a way of representation, but also a convenient tool to analyze and reason about the system performance [14]. Reasoning in MFM models is based on dependency relations between states of objectives and functions.

3.2.1 MFM Function States

Each function can be either enabled or disabled. For any enabled function, the possible states are listed in Table 3 Note that the disabling of a function is not another state of the function, but it means that the function will no longer be available for the system. For example, a no-flow transport is different from a disabled transport.

3.2.2 MFM Causal Roles

The casual roles in MFM represent how non-transport functions influence the upstream or downstream flow within a flow structure. To demonstrate how to use causal roles in MFM modeling, the previous cooling system is used.

The flow structure «mfs1» in Fig. 4 representing the functions of the fresh water loop contains two functions: «sto2» and «tra4». The mass flow rate represented by the state of «tra4» is determined by an active pump. Therefore, «sto2» is connected by a participant role to «tra4» both from upstream and downstream direction, (meaning that the flow rate is independent on the state of the storage function). However, in «mfs2», «sto3» that represent the storage function of water tank, has the potential to influence the downstream injection of water into the sea water loop. Therefore, «sto3» is connected with an influencer role with the downstream transport «tra8».

3.2.3 MFM patterns

Based on the function states and the causal relations between different functions, reasoning rules can be defined for a generic set of MFM reasoning patterns summarized in Table 4. The rules are derived from the pattern by the following principle: If either the transport function states or the non-transport function state is known (gray) or can be assumed, then based on the causal roles, a hypothesis of the other function states can be inferred.

In a complete MFM model, the reasoning can start at whichever function in the model, and propagate to an end-node in the model through various MFM patterns. It should be noted, that for each MFM reasoning pattern, not only a prediction can be made (about a possible consequence) but also a post diction (a possible cause) can be drawn from a function state. Using the storage pattern for example, one may draw two conclusions from a storage-influencer-transport pattern assuming that the storage is in low volume state: 1) The consequence may be that the downstream transport will have a low flow rate; and 2) The cause may be that the downstream transport had a high flow rate. Reasoning about causes and consequences are separate processes, the former is reasoning forwards in time and the latter backward.

The latest version of the MFM causal reasoning rules for both causes and consequences reasoning are presented in [15]. The reasoning rules and the inference mechanisms are implemented using a rule-based reasoning system which is integrated with a model editor in the MFMSuite [13].

3.2.4 Diagnosis of ship engine cooling system

We will use the model in Fig. 4 to demonstrate diagnostic reasoning in MFM reasoning. The reasoning results will be compared to the fault tree analysis. For the purposes of comparison, the energy removal is selected as the starting point of the reasoning. The state of «tra1» in the model is specified as low flow and the fault diagnosis is run by using the MFM model. Three primary possible causes are deduced by the reasoning engine: 1) the closed loop water circulation is in fault condition («tra4»), 2) the heat exchanger in the energy level is fault condition («bal1»), and 3) the sea water loop is in fault condition («bal2», «tra5», «tra10», and «sou3»).

One of the causes was been analyzed in Section 2 namely that the loss of energy removal capability is caused by a lack of energy flow from the heat exchanger to the sea (low flow in «tra3»). One of the causes for this may be that the primary pump cannot serve its function to transport the water in the sea water loop (low flow in «tra5»). From «tra5», the reasoning can be continued to trace the energy conversion within the pump. The reasoning path produced by the reasoning system is: (“>” means “can be because of”)

Objective (false)
>Overall Energy Level {tra1(low) > sto1(high)>tra2(low)>tra3(low)}
>Water Mass Level {tra6(low)>tra5(low)}
>Pump Energy Level {tra15(low)>sto6(low)>tra14(low)>sou5(low)}

It is seen that the reasoning result from MFM model corresponds to the analysis presented in Section 2. The fault trees (and consequence trees) is generated by the MFM reasoning by interpretation of an initial event using the rules and model. Note that MFM reasoning will generate all possible cause and consequence paths which can be derived from and consistent with the means-end relations included. The first principles of operation embedded in the MFM model ensure both consistency and completeness (within the scope of the model).

4 Nuclear Power Plant Applications

MFM has been used for both reliability analysis and for diagnosis nuclear power plants. Yang et. al. [16] use MFM for reliability studies of nuclear power plants and demonstrate that MFM can be used to generate fault trees which are more complete than those produced by traditional manual procedures. Zhang[15] (the second author of this paper) has developed a comprehensive MFM model of the primary coolant loop of a PWR to be used together with the MFM reasoning system in a pilot experiment on diagnosis with the Ringhals simulator at OECD Halden, Norway. Lind et.al. [17] developed an MFM model of the FBR Monju demonstrating the use of MFM to model a nuclear power plant and its associated control systems. The PWR and FBR studies summarized below demonstrate the ability of MFM models to represent the complexity of nuclear power plants. The PWR study show demonstrates the modeling procedure described above for a complex system. The FBR study demonstrates how decomposition and reuse strategies can be used to reduce the modelling effort.

4.1 Model of a PWR primary system

The PWR primary system considered in [17] includes three Reactor Coolant Loops (RCL) as shown in Fig. 6. Each RCL contains a Steam Generator (SG), a Reactor Coolant Pump (RCP) and a cold-leg collector (CC) connected to the main circulation pipeline. The pressurizer surge line is connected to the second RCL. The system also includes a Chemical and Volume Control System (CVCS), and a safety injection system. In the modeled unit the low pressure safety injection pumps are combined with residual heat removal pumps, and the high pressure injection pump is combined with the inlet charging pump from the CVCS. The control rods, which are not illustrated in the diagram, are also included in the modeling. In the following, a step by step explanation is provided which demonstrate

the MFM modeling of a PWR system.

According to the modelling procedure in section 3.1.3, objectives and mass/energy flows need to be determined first. The main operational objective for the PWR primary system is to generate and transport energy (in the form of heat). This objective is achieved by transporting the heat produced in the reactor to the SGs. The energy will be further transported from the primary side coolant loop to the secondary steam line inside the SGs. The energy is transported by means of the water circulation in the RCLs. The objectives can be summarized as 1) maintain heat production, 2) maintain delivery of produced heat for power production, 3) maintain water level in RCS, 4) maintain water circulation in RCS, 5) maintain the average temperature and pressure (energy level) in the system.

Two major flow structures (one energy flow and one mass flow) can be easily identified. Furthermore, two means of influencing the reactivity and thereby the energy production in the system: one means is to move the control rods, and the other is to inject boron through the CVCS. The functions of these two means of influencing energy production can be represented by two additional mass flows structures.

Considering the energy flow structure «RC_energy», the reactor is considered to be a source of energy, and two energy sinks can be identified. The first energy sink is the function provided by the secondary system (which uses the heat generated in the reactor to produce steam, which in turn moves the turbine to generate electric power and deliver the power further into the grid). The second energy sink is the function provided by the emergency cooling system. The model of the energy flow is shown in Fig. 7. Note that the function names of the partial models shown in the figures are not definite, they may vary from the final complete model shown in Fig. 10.

The flow function «tra44» represents the transportation of the generated heat from the primary to the secondary side during normal energy production. The remaining heat will be circulated back to the general energy storage represented by «sto_heat» through the cold legs. During emergency situations, when the function «sin_pp» is not available, the energy is removed through «sin_em», by using the facilities for emergency cooling.

The mass flow structure can be considered as a closed system during operation and modelled only using different storage functions representing the water storage capacity of the reactor vessel, the SGs, CCs and the pressurizer. Fig. 8 shows an MFM model of the RCLs with the pressurizer. The transport function «tra_ps» represents the function of pressurizer spray line.

However, from an operational perspective, the Reactor Coolant System (RCS) is failing when any single cooling loop fails to meet the operational requirements. From a functional perspective it is therefore reasonable to represent (through abstraction) the three reactor cooling loops as one coolant loop. This offers a simpler model with full representation of the RCS functions. The functions of the make-up system is not considered in this study, so the CVCS can be considered as the water storage with an open loop from a source to a sink (omitting the recycling of the boron and water) that is connected directly to influence the water level in the RCS. So in the general model, the CVCS and the RCS can be represented in MFM as in Fig. 9. The water storage function of the VCT tank is represented in Fig. 9 by «sto_vct». Additionally, another source can be considered in the mass flow,

namely the function of the Reactor Water Storage Tank (RWST). There is also another sink function which is realized by the Pressurizer Relief Tank (PRT).

After the partial models of the PWR primary have been developed, they can be combined with a few modifications (adding additional storages, balances, and transports) to produce a complete MFM model of the PWR including the means-end relations between the flow structures. A complete MFM model of the PWR primary side is shown in Fig. 10. Notice that four additional energy flow structures not mentioned above have been added to the model namely the energy flow structures «efs2», «efs3» and «efs4». They represent the energy flows within the RCPs, the high head safety injection pump (also used as CVCS charging pump), and the low head safety injection pumps (also used as Residual Heat Removal Pumps), respectively.

Boron injections and control rods insertions are represented by with separate mass flow structures «mfs2» and «mfs3». Here we consider the storage function as the total amount of boron or inserted rods, which influences the reactivity in the reactor. Transport functions from the source and to the sink represent the process of injection and removal, respectively.

The main function in each of these three energy flow structures provides the means to transport water in different parts of the coolant mass flow in «mfs1». For the purpose of demonstration, an additional function of the charging pump is also modelled in Fig.10, which is to provide the pressure for RCP seals. In the Fig 10 «bar1» is a barrier representing the seal function which is conditioned by the pump energy flow. However, during normal operation, the water flow through the pump seals is too small to make an impact on the system function, and thus can be neglected during the modelling.

A fourth energy flow structure not yet mentioned is «efs5», which represents the pressure control function of the pressurizer. The pressurizer is an important component of the PWR system and requires a detailed energy balance representation. The energy flow structure «efs5» is overlapping with «efs1» because the function of the pressurizer is to control the pressure of the whole primary system. Therefore, «efs5» can also be viewed as a detailed representation of «sto8» in «efs1». Because it has been decided to model the pressurizer vapor phase («sto20») and liquid phase («sto22») separately in «efs5», in order to represent the functional aspects of the thermal dynamic, the function of the pressurizer represented in the mass flow structure «mfs1» is also decomposed into vapor storage and liquid storage. Between the mass flow and energy flow structure of the pressurizer dynamic, the energy accumulated together in the two different phases drives the phase transitions, while at the same time energy is transported alongside with the phase changes. The MFM means-end relation producer-product is used to describe the influence from energy storages «sto20» and «sto22» to the mass transports «tra6» and «tra5», while the MFM mediate relations are used to describe the influence from the mass transports «tra6» and «tra5» to the energy transports «tra52» and «tra51».

The objectives summarized in the beginning of Section 4.1 can be correlated with the objectives represented in Fig. 10. Objective 1 and 2 are represented by «obj2» and «obj5». Objective 3 and 4 are represented by «obj4» and «obj3» and objective 5 is represented by «obj6».

Note that decomposition is done in the model, for example the storage («sto13») and balance («bal3») functions are added to fully describe the function of the CCs in the system. However, the model

presented in this section is still a highly abstract functional representation of the process, but it serves well for the purposes of demonstrating the modelling capability of MFM. The ability to choose the level of abstraction which fit the purpose of the model is one of MFM's features which make it attractive for dealing with complexity.

The causal relations between different functions within a flow structure allow the model to be used for causal reasoning as explained in Section 3.3.

4.1 Modeling a FBR

The second nuclear power plant modelling example is the MFM model developed of the FBR Monju [17]. This model was developed by a decomposition strategy which increased the efficiency of the modelling process. The basic combined top down and bottom up modelling approach illustrated with the PWR example can be very costly and strategies which can reduce the modeling effort are highly desirable and even necessary for practical applications. The FBR modelling also included representation of the function of control systems. Interested readers are referred to [17] for detailed explanations of the modeling strategy and the representation of control systems. Here we will only summarize the modeling strategy used for decomposition which has features which can be generalized to other types of nuclear plants and processes in other engineering domains where MFM is used (e.g. in oil and gas).

The MFM model of the FBR Monju was built by decomposing the plant into the following three subsystems

- Primary heat transfer system (PHTS)
- Secondary heat transfer system (SHTS)
- Energy conversion system (ECS)

Each subsystem and the included components will be defined below.

Note that this decomposition into systems is reflected neither in a P&I diagram of the plant nor in the MFM model. The P&I decompose into components or equipment and MFM decompose into levels of function. Functions and components are related by many to many mappings i.e. models of functions and components are not isomorphic. A decomposition of the plant into components accordingly cannot address functional constraints (and the reverse). The three subsystems PHTS, SHTS and ECS correspond to the decomposition used by the plant engineers and operators.

It is shown in [17] that the decomposition of the FBR Monju into three subsystems suggested above it is possible to use an MFM model of a generic heat transfer loop as a template for building MFM models of the PHTS and the SHTS subsystems. But since the subsystems do not strictly match the functional decomposition of MFM "partial" or incomplete function structures have been applied when representing subsystem functions (see [17] for details). However, even though the function structures for the PHTS systems, the SHTS system and ECS are incomplete they can be directly combined into the "complete" function structures of MONJU shown in Fig. 11. Below we will provide brief

descriptions of each of the sub-models. The control functions included in the modes will not be described. The reader is referred to [17] for details.

4.1.1 Primary heat transfer system PHTS

The components in the primary heat transfer system PHTS includes the reactor with control rods, the CRMD controller, the reactor power controller, the sodium coolant, the IHX heat exchanger, the PHTS circulation pump, the PHTS circulation pump controller and the PHTS flow controller. The MFM sub-model of the PHTS system is shown in Fig. 11. The PHTS sub-model contains three functional levels efs1, mfs1 and efs4. The functions in structure efs1 represent the pumping and hydraulic functions of the PHST involved in the conversion of electrical energy to rotational and kinetic energy in the hydraulic circuit. The structure mfs1 represents the storage (sto4) of sodium in the core and its circular transportation (tra10) and includes also a source sou4 representing the radioactive material in the core and two barrier functions bar1 and bar2. The barrier bar1 represents the function of the cladding. The barrier bar2 represents a function of the IHX heat exchanger which is to separate the primary and the secondary coolant media so that radioactive materials in the PHTS coolant is prevented from entering the SHTS system. The structure efs4 represents the delivery (sou5), transfer (tra21) and storage (sto7) of energy in the reactor coolant circuit. The transfer of energy from the PHTS to the SHTS mediated by the circulation of coolant is represented by tra22 including its connection with tra10 in mfs1 by a mediation relation.

4.1.2 Secondary heat transfer system SHTS

The components in the SHTS subsystem include the IHX heat exchanger, the SHTS circulation pump, the evaporator EV and the super-heater SH. The main purpose of the SHTS system is to transfer energy from the PHTS system to ECS. The MFM sub-model of SHTS system is shown in Fig. 11. The SHTS sub-model includes three barrier functions bar2 and bar3 and bar4. These three barriers represent safety functions of the SHTS which is to prevent the transfer of radioactive material between the PHTS and the ECS (through the evaporator EV and the super-heater SH). In function structure efs4 representing the energy transfer function (tra23) of the SHTS system we have included a storage (sto8) representing the storage of heat in the coolant and the components in the SHTS circuit.

4.1.3 Energy conversion system ECS

The main components of the energy conversion system includes the evaporator EV, the super heater SH, the moisture separator, the feed water pump, the turbine generator and the condenser and the condensate pump. The functions of these components are highly interacting and the MFM sub-model of the ECS is by far the most complex of the three sub-models in Fig.11. The functions in efs3 and is similar to efs2 describing the functions of the SHTS. The energy aspects of the pumping are represented by efs3. The power supply to the feed water pump is represented by sou3, the energy conversion to kinetic energy of the feed water is represented by tra8 and by tra9 which represents the losses due to pressure drops in the circuit including the pressure drop caused by the feed water control valve. Considering the mass flow structure mfs1, a natural place to start is at the transport function tra18 which represents the transportation of feed water by the pump. The balance bal1 located upstream tra18 represents the balancing of the feed flow with the output flow (tra12) to the moisture

separator performed by the evaporator (EV). The separation is represented by the balance function bal2 and the three transport functions tra19, tra14 and tra15. The water separated from the steam (tra19) is returned to the main feed water line. This is represented by bal4 which combines the flow from the condenser pump (tra20) with the separated water (tra19). The transportation of superheated steam produced by SH is represented by tra14 and is used for control. The transport tra15 represent the transportation of steam from the evaporator output directly to the point (bal3) where it is mixed with the superheated steam. From bal3 there are two flow paths represented by tra16 and tra17. These functions represent the turbine (tra16) and the bypass line to the condenser whose function is represented by sto6 since its purpose is to collect the water condensed by the turbine and the bypass flow.

The balance function bal5 in efs4 represents the aggregated function of the SHTS side of the evaporator EV and the super-heater SH. The two energy transport functions tra24 and tra25 represent the energy transferred from the SHTS to the secondary sides of the evaporator (tra25) and the super-heater (tra24). The energy accumulation in the evaporator and super-heater are represented by sto9 and sto19 and tra26 and tra27 represent the energy transfers from the EV and the SH to the turbine by the steam. The conversion of energy in the turbine-generator is represented by tra28, bal6, tra29 and tra30. Transport tra29 represents here the transfer of the electric energy generated by the generator to the grid represented by the sink function sin8. Transport tra30 represents the transfer of energy to the condenser which here for simplicity is represented as sin9.

5 Conclusions

The paper presents functional modelling and its application for diagnosis in nuclear power plants. Functional modelling is defined and it is relevance for coping with the complexity of diagnosis in large scale systems like nuclear plants is explained. The diagnosis task is analyzed and it is demonstrated that the levels of abstraction in models for diagnosis must reflect plant knowledge about goals and functions which is represented in functional modelling. Multilevel flow modeling, which a functional modelling methodology is introduced briefly and illustrated with a cooling system example. The use of MFM for reasoning about causes and consequences is explained in detail and demonstrated by the cooling system example. MFM modeling applications in nuclear power systems are described by two examples a PWR and a FBR reactor. The PWR example describes a top down modeling approach and the FBR example show how the modeling development effort can be reduced by proper strategies.

Acknowledgment

The work was supported by the Chinese 111 project on Nuclear Safety and Simulation hosted by CNST at Harbin Engineering University, and by the IFE OECD Halden Reactor Project in Norway through the co-funding of Xinxin Zhang’s PhD project and the joint development of the MFMSuite.

References

[1] IAEA, "On-Line Monitoring for Improving Performance of Nuclear Power Plants Part 2: Process and Component Condition Monitoring and Diagnosis", International Atomic Energy Agency report No. NP-T-1.2., 2008.

[2] M. Lind "Modeling Goals and Functions of Complex Industrial Plants." *Applied Artificial Intelligence*, vol. 8(2), pp. 259-283 (1994).

[3] M. Polanyi, *Personal Knowledge*, Routledge Kegan Paul, London England, (1962).

[4] M. Bunge, *Treatise on Basic Philosophy Vol 2- Semantics II: Interpretation and Truth*. Dordrecht, Holland: D. Reidel Publishing Company (1974).

[5] S.S. Jørgensen, "Fault diagnosis using generic Multilevel Flow Modelling Models." PhD thesis (93-A-700), Institute of Automatic Control Systems DTU, 2800 Kgs. Lyngby Denmark. 1993.

[6] Lind, M., "Introduction to Multilevel Flow Modeling," *International Journal of Nuclear Safety and Simulation*, vol. 2(1), (2011).

[7] M. Lind, "An Overview of Multilevel Flow Modeling," *International Journal of Nuclear Safety and Simulation*, vol. 4, pp. 186-191 (2013).

[8] Lind, M., "Control Functions in MFM, " *International Journal of Nuclear Safety and Simulation*,.

[9] M. Lind, "Knowledge Representation for Integrated Plant Operation an Maintenance," *Proc. 7´th ANS Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies NPIC&HMIT2010*, Las Vegas, Nevada, November 7-11, (2010).

[10] A. Gofuku, "Applications of MFM to intelligent systems for supporting plant operators and designers: function-based inference techniques," International Journal of Nuclear Safety and Simulation, vol. 2(3), (2011).

[11] Lind, M. and Zhang, X.,"Applying Functional Modeling for Accident Management of Nuclear Plant," accepted for publication in *International Journal of Nuclear Safety and Simulation* (September issue 2014).

[12] K. Heussen and M. Lind, "On support functions for development of MFM models," Proc. First Int. Symposium Socially and Technically Symbiotic Systems, August 29-31 2012, Okayama Japan, (2012).

[13] Thunem, H. and Zhang, X. "Advanced Control and Automation Support; Continued Development of the MFMSuite. Proc. Enhanced Halden Programme Group Meeting, HWR-1117, Røros Norway, June 2014.

[14] M. Lind. "Reasoning about Causes and Consequences in Multilevel Flow Models," *Proceedings of ESREL 2011*, Troyes France, September, (2011).

[15] Zhang, X., Thunem, H., Lind, M., Jørgensen, S. B. and Jensen, N. "Practical application of the MFM Suite on a PWR simulator: modelling and reasoning on causes and consequences of

process anomalies," Proc. Enhanced Halden Programme Group Meeting, HWR-1118, Røros Norway, June 2014.

[16] M. Yang, Z. Zhang, M. Peng and S.Yan. "Modeling Nuclear Power Plant with Multilevel Flow Models and its Applications in Reliability Analysis." *Proc. Int. Symp. on Symbiotic Nuclear Power Systems for the 21´th Century (ISSNP)*, Tsuruga Japan, July 9-11 (2007).

[17] M. Lind, H. Yoshikawa, S. B. Jørgensen, M. Yang, K. Tamayama and K. Okusa, "Multilevel Flow Modeling of Monju Nuclear Power Plant," *Proc. ICI2011*, Daejon Korea (2011).M. Lind, H. Yoshikawa, S. B. Jørgensen, M. Yang, "Modeling operating modes for the MONJU nuclear power plant," *International Journal of Nuclear Safety and Simulation*, vol. 3(4), pp. 314-324 (2012).

Table 1. The significance of plant states depends on the plant goal in view. Each state interpretation is associated with the remedial task to do. For each task there is a set of corresponding actions.

Sensor value	State (meaning)	Goal	Remedial Task	Remedial Action
dP is zero	S4:Engine cooling is lost	G4:Maintain engine temperature within limits	T4:Restore energy balance	A4:Reduce energy production
	S3:No flow of seawater	G3:Maintain coolant flow	T3:Restore coolant flow	A3:Reconfigure and start auxiliary cooling system
	S2:Pump P2 is not doing mechanical work	G2:Produce pressure	T2:Restore pressure	A2:Reconfigure and start P3
	S1:The pump motor has stopped	G1:Keep pump running	T1:Restore pump revolutions	A1:Start pump motor

Table 2. Basic MFM symbols

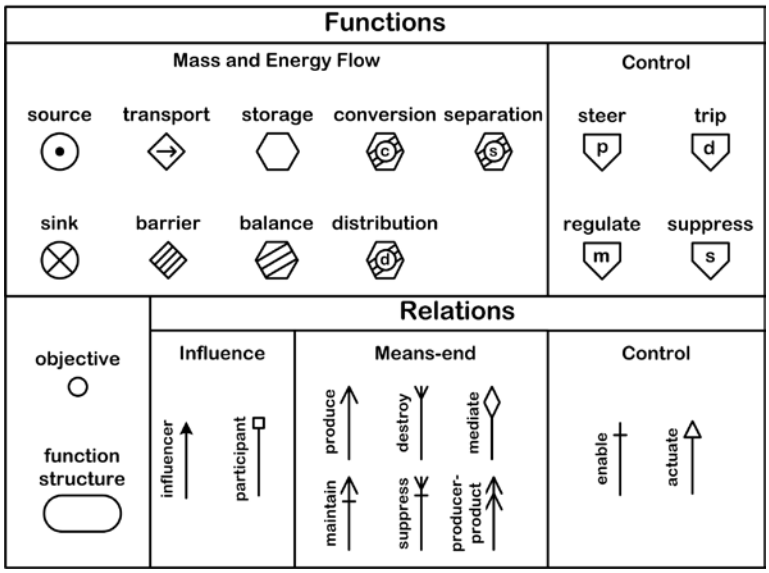
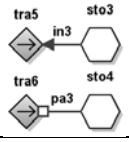
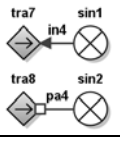
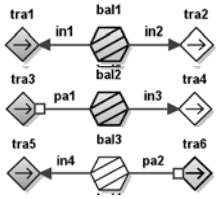
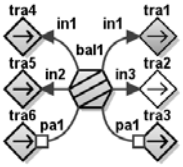
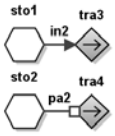
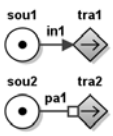


Table 3. States of MFM functions

Function/Target	Normal State	Abnormal State			
balance	normal		leak	block	sourcing
barrier	normal		leak		
transport	normal	low-low	low	high	high-high
sink	normal	low-low	low	high	high-high
source	normal	low-low	low	high	high-high
storage	normal	low-low	low	high	high-high
objective	normal	false			
threat	normal	false			

Table 4. MFM reasoning patterns

storage	sink / source	balance	
			
			

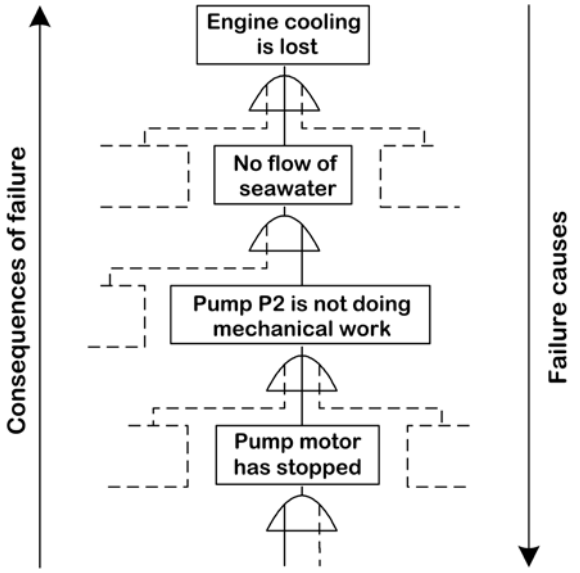


Figure 1. Example fault tree for the ship engine cooling system

.

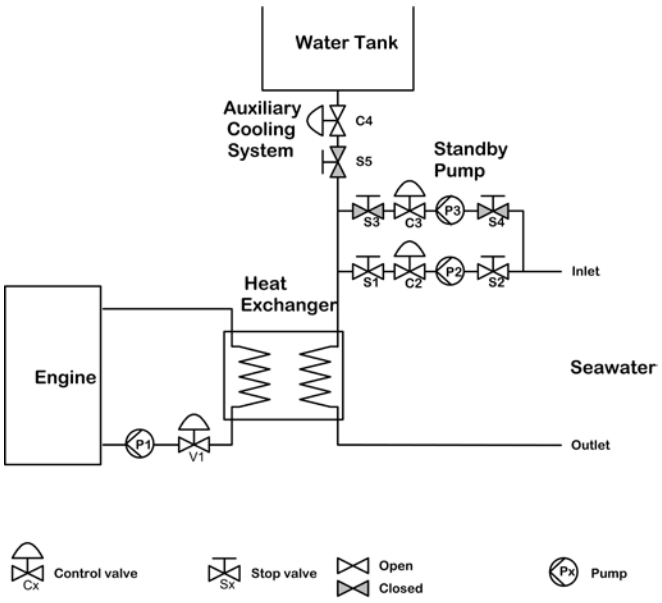


Figure 2. The ship engine cooling system

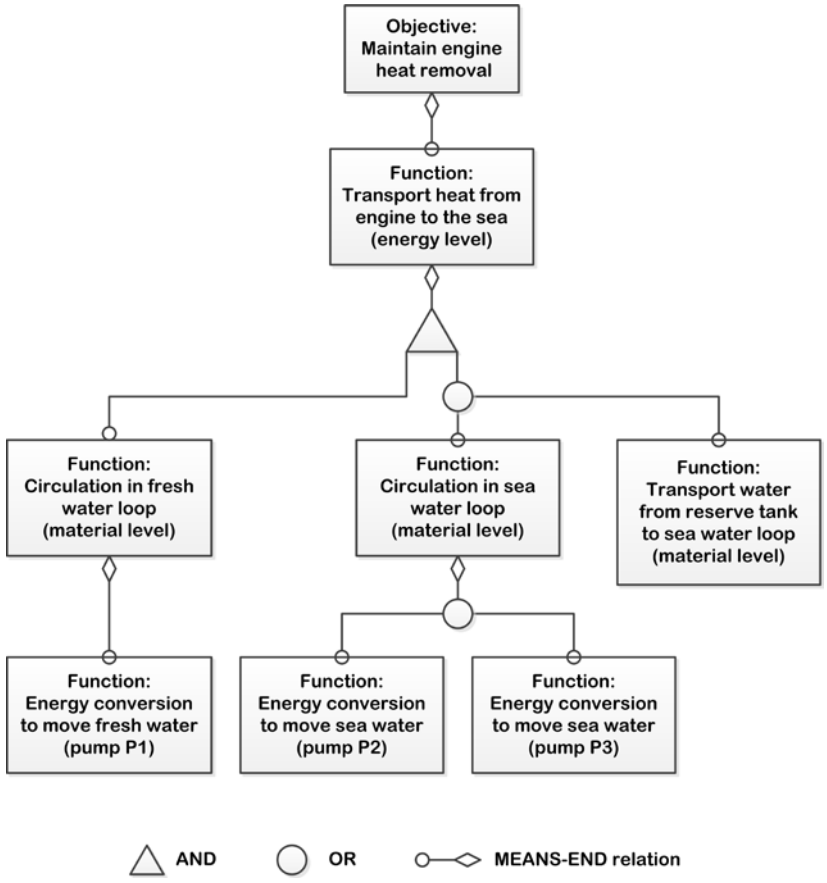


Figure 3. Means-end analysis for the ship engine cooling system.

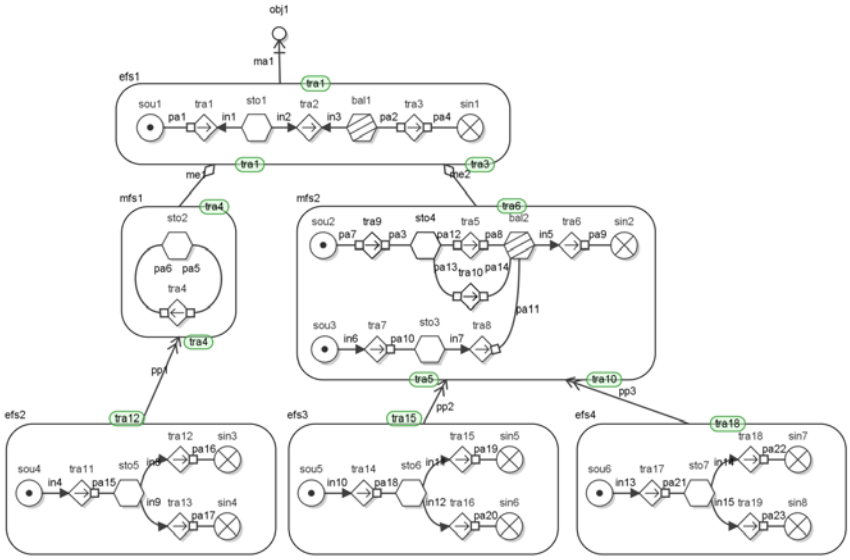


Figure 4. Means-end analysis for the ship engine cooling system.

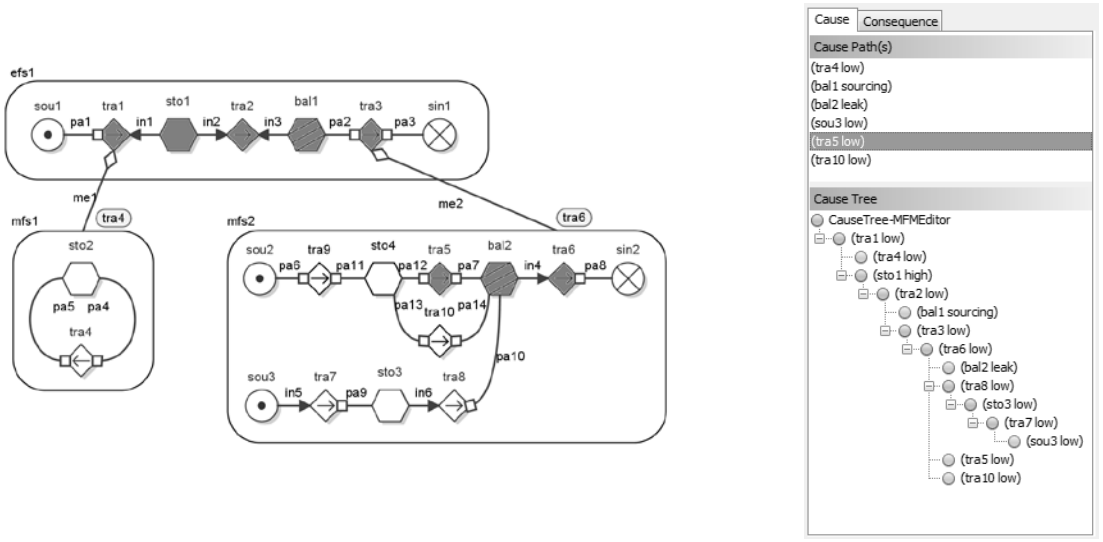


Figure 5. Reasoning result.

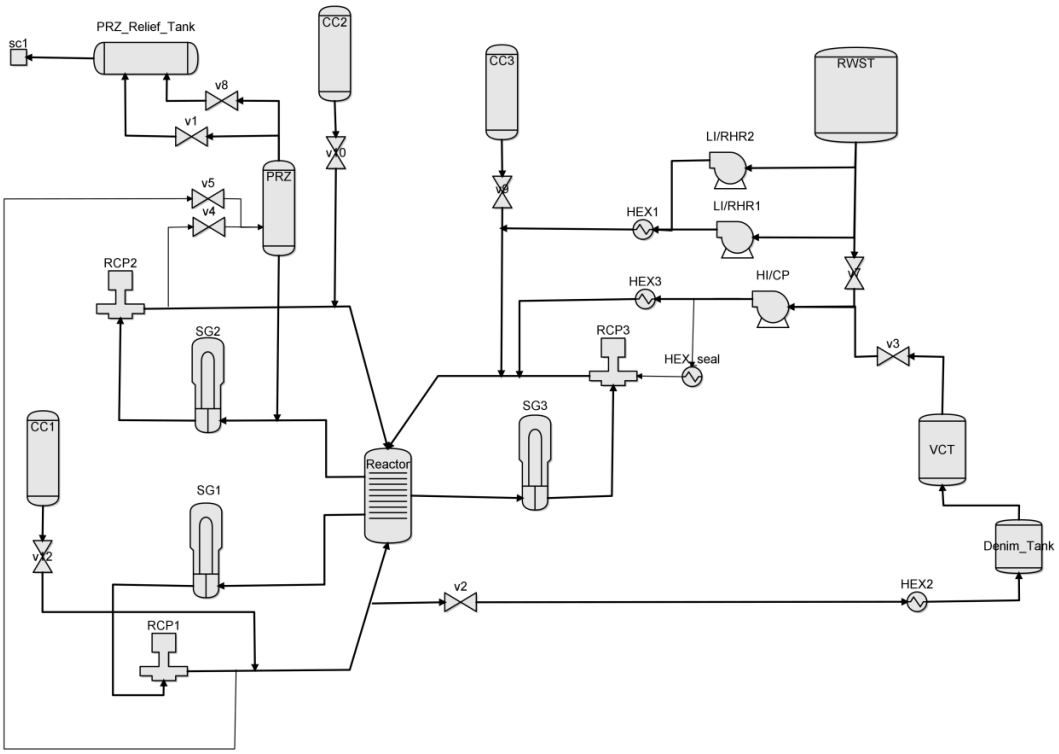


Figure 6. The primary side of the PWR system (with the safety injection system) to be modelled.

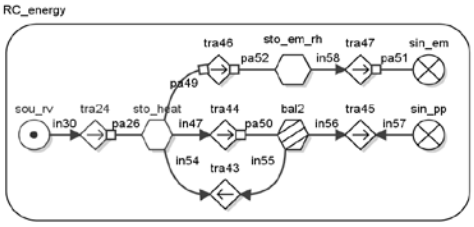


Figure 7. MFM model of the primary side energy flow.

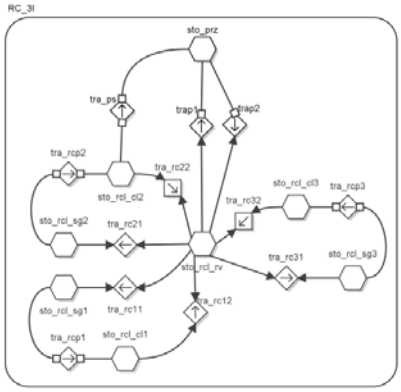
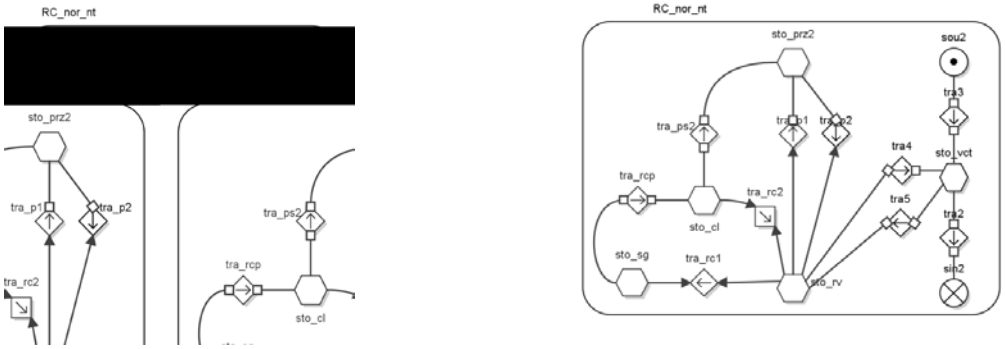


Figure 8. MFM model mass flow of three RCLs and pressurizer.



RCS system RCS and CVCS

Figure 9. Abstract MFM mass flow structures of RCS an CVCS systems.

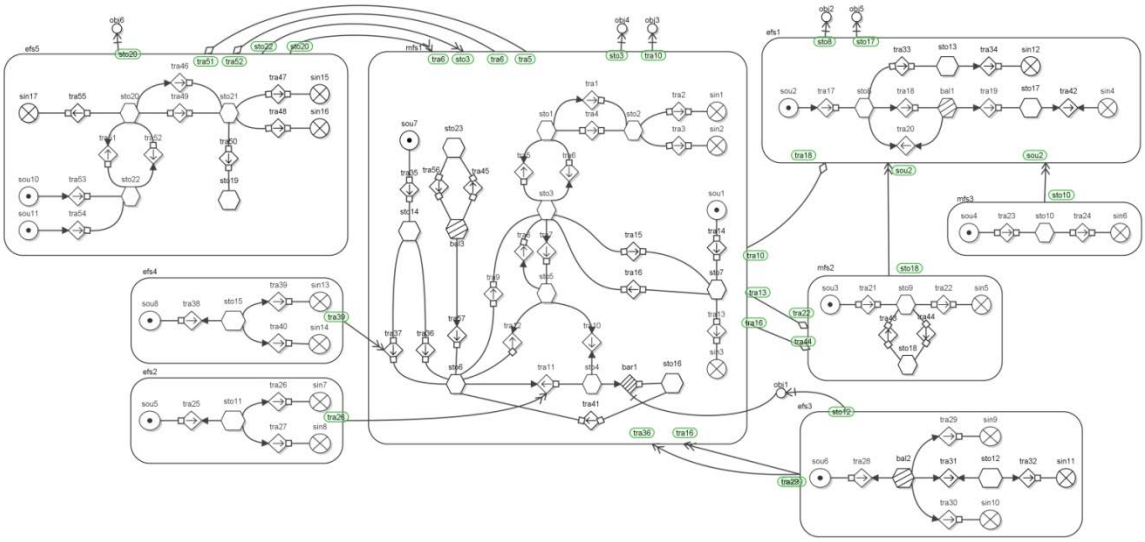


Figure 10. A complete MFM model of the PWR primary system.

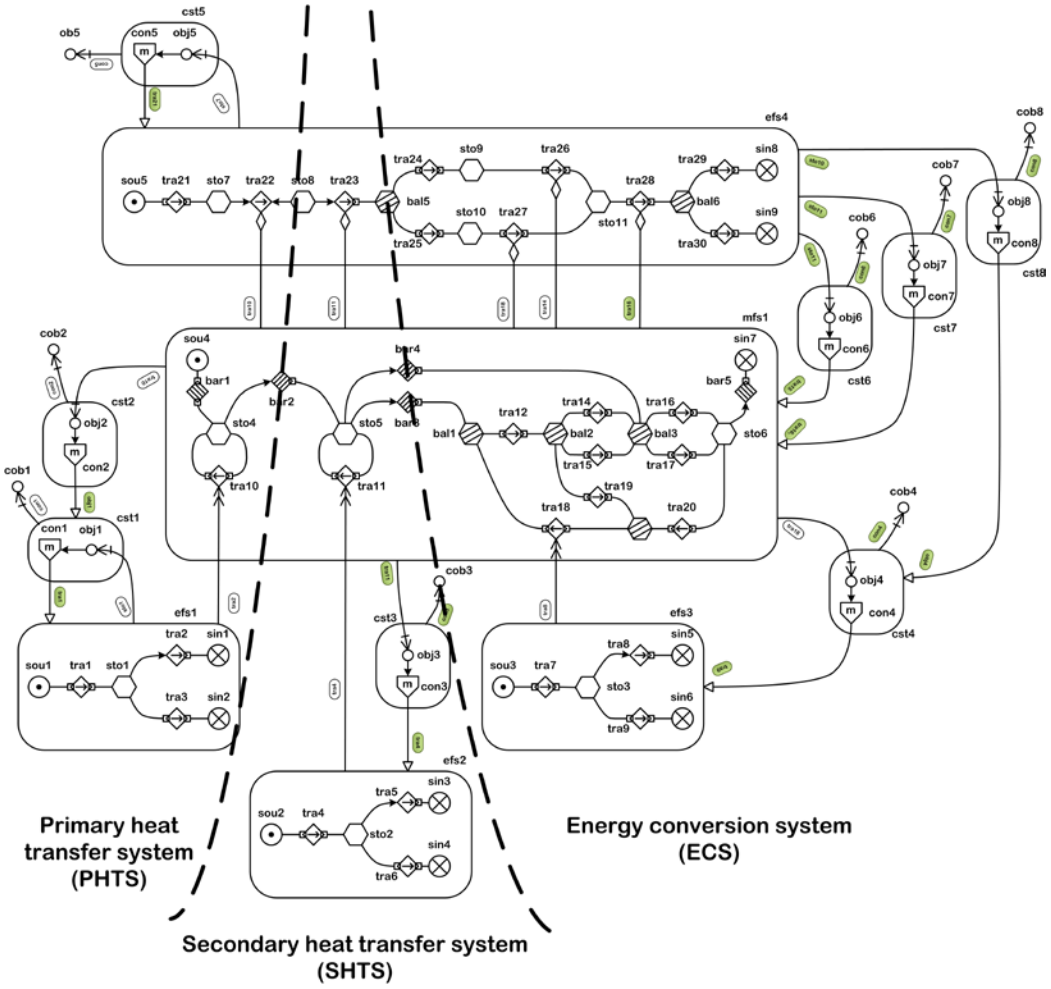


Figure 11. MFM model of the FBR Monju.